图书情报工作
第64卷 第19期 2020年10月

大数据环境下安全情报工作协同研究*
——以反恐情报工作为例

■ 安璐[1,2] 周亦文[2]
[1] 武汉大学信息资源研究中心 武汉 430072 [2]武汉大学信息管理学院 武汉 430072

摘 要：[目的/意义]大数据环境对安全情报工作协同提出了更高的要求，研究安全情报工作协同中的问题及其方案有助于安全情报相关部门通力合作，提升安全情报工作的成效。[方法/过程]对大数据环境下安全情报工作协同可能遇到的问题进行探讨，以反恐情报为例，结合情报工作的流程，分析安全情报工作的主体与协同需求，提出反恐情报工作协同方案。[结果/结论]提出的反恐情报工作协同方案为：在反恐领导小组发布的反恐情报需求指引下，公安部等专业部门协同中国人民银行、交通运输部、工业和信息化部、海关总署等一般业务部门及金融业、运输业、电信业、医疗和非营利性部门及群众等社会力量开展特定领域反恐情报的搜集、处理、分析、应用与反馈。

关键词：安全情报 反恐情报 协同 情报流程 大数据
分类号：G203
DOI：10.13266/j.issn.0252-3116.2020.19.006

1 引言

安全情报是指对安全管理产生影响的安全信息[1]。安全情报工作有助于维护国家安全与社会稳定。2017年10月18日，习近平总书记在中国共产党第十九次全国代表大会上指出“坚持总体国家安全观。统筹发展和安全，增强忧患意识，做到居安思危，是我们党治国理政的一个重大原则。必须坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，完善国家安全制度体系，加强国家安全能力建设，坚决维护国家主权、安全、发展利益。”根据国家总体安全观的内涵，国家安全情报体系应当是一个协同的有机统一整体[2]。在总体国家安全观下，通过情报共享与协同发挥规模优势是一项隐性要求[3]。

大数据具有体量大、类型多、速度快和价值密度低的特点。它既给安全情报提出了挑战也带来了机遇。一方面大数据能够提供丰富的情报，另一方面传统的情报工作方法也不完全适用于大数据环境下的安全情报工作。大数据环境下的安全情报工作不仅依赖于专业的情报工作者提供安全情报，同时也需要从各行各业的海量数据中提取安全情报。情报来源的多样化使得安全情报流程更加复杂，如果缺乏有效的协同不仅容易造成重复劳动，而且单独的业务部门或情报部门可能面临专业知识与技能不足，影响情报工作的成效。协同的安全情报流程能够提高安全情报工作的效率，做到知识与技能的交流与共享，节省情报工作的时间和物质成本。在合作过程中，多数协同问题的根源是“如何协同”的问题[4]。因此在安全情报工作中，有必要从情报流程的角度进行安全情报工作协同研究。

“安全情报”这一概念涉及的领域包括国家安全、公共安全和生产安全[5]。与反恐任务相关的组织所需要的情报被称为反恐情报[6]。反恐是美国国土安全部的职责之一[7]，中国也将反恐纳入国家安全战略[8]。因此，反恐工作是一项国家安全工作，反恐情报属于安全情报中的一种。反恐情报与安全情报的不同点在于二者涉及的领域范围不同，安全情报涉及的领域更广，

* 本文系教育部哲学社会科学研究重大课题攻关项目“提高反恐怖主义情报信息工作能力对策研究”（项目编号：17JZD034）和国家自然科学基金重大课题“国家安全大数据综合信息集成与分析方法”（项目编号：71790612）研究成果之一。
作者简介：安璐（ORCID：0000-0002-5408-7135），数据管理与知识服务研究室主任，教授，博士生导师，E-mail：anlu97@163.com；周亦文（ORCID：0000-0001-9709-5568），博士研究生。
收稿日期：2019-12-15 修回日期：2020-04-21 本文起止页码：50-60 本文责任编辑：易飞

反恐情报仅涉及反恐工作。

本文以反恐情报工作为例,从情报流程的角度对安全情报工作协同进行研究,针对反恐情报的特性,详细分析其情报流程各环节中具体的协同问题,并构建反恐情报流程协同方案。

2 相关研究

2.1 安全情报

安全情报是融合了情报学与安全学的综合学科[9]。现有的安全情报研究主要是关于安全情报法律体系、安全情报方法、安全情报体制等方面的研究。例如,王秉等从安全科学的学理角度对安全情报的概念和演变趋势进行了探讨[5],并提出情报主导的安全管理的概念模型和实施模型[10]。高金虎[11]指出要打造一体化的国家安全情报工作机制,并提出国家安全情报体制的改革路径。章雅蕾等[12]论述了总体国家安全观背景下安全人员的必备素养,即安全情报素养。安全情报素养是指对安全情报的获取、分析和利用的能力[13]。秦殿启等[14]指出在大数据环境下安全情报人员的情报素养对信息安全十分重要,情报人员应具备开放性、发展性和互动性。李辉等[15]指出在国家安全情报工作中,情报感知分析需要考虑海量的信息和复杂的环境,情报人员的情报感知分析能力和工作强度都面临巨大挑战。

尽管目前学者们从不同角度对安全情报相关的问题进行了探讨,但较少有学者结合大数据环境的特点对安全情报工作的协同进行研究,从情报流程的角度对安全情报工作的具体协同机制的研究也显得不足。

2.2 情报流程

情报流程是开展情报工作的基本程序,其重要性不言而喻。情报流程是指一系列情报工作的步骤或阶段[16],也可以表述为以特定阶段为核心的若干阶段[17]。情报流程有利于明确在不同的阶段进行情报工作的人员构成和工作目的。明确详细的情报流程可以提升组织的信息搜集能力和决策能力,并借此提高组织的竞争能力[18]。

目前并没有形成对情报流程的统一认识,学术界提出了多种模型,包括线性推进模型、情报周期模型、多重反复模型、网络交互模型、目标中心模型等[19]。R. Chakraborty 等[20]通过采访调查印度警方,指出情报流程对于恐怖袭击中危机管理的积极作用。A. Williot 等[21]同样指出流程策略能极大地影响警方危机检测的能力。李建辉等[22]对公安情报流程进行了研究,将其分为数据挖掘、数据管理、分析预测、情报产品分发与反馈 4 个阶段。F. Bartes 在总结前人研究的基础上,提出了反竞争情报循环,并将其划分为规划和引导、数据收集、分析、行动与评估 5 个阶段[23]。

现有研究大多是从情报活动环节的角度针对情报流程进行研究,使用高度概括的模型对情报流程进行描述。这类研究虽然具有普适性,但在应用到具体领域时缺少专业性。目前有关情报流程的研究中,鲜有针对反恐情报流程的研究。有部分研究者研究了与反恐情报流程类似的公安情报流程。反恐情报与公安情报虽然相似,但也有其特殊性。反恐情报活动是需要全民参与的活动,因此其情报主体的构成比公安情报更加复杂,是一个复杂的、涉及多个部门的任务。反恐情报的用户需求比公安情报的用户需求更加多样化。目前的研究没有从情报流程的角度考虑反恐情报工作的协同。而协同的流程,通过职能互补、合作和资源共享可以提高效率、取得利益最大化。

2.3 协同理论

为了更好地完成安全情报工作,我们需要建立一个敏锐的、能够应对多方威胁的、达到良好协同效果的情报组织网络。T. W. Malone 等将协同定义为和谐的合作,并指出为实现整体目标,对信息进行合理共享的方式是协同中最重要的问题之一[24]。在组织中,协同是组织提升竞争力的关键因素[25]。对于组织而言,协同是指各部门之间通过相互配合,使得总体价值大于各部分价值之和。"协同"并非只是两个组织之间的合作,而是两个组织之间的优势互补、互利共生[26]。协同学认为如果组织没有形成良好的协同体,组织会陷入无序、混乱的状态[27]。整体政府理论是政府部门协同的重要理论之一。整体政府理论强调通过整合与协调,建立跨组织的协作,优化政府职能。整体政府理论不仅强调各组织在目标一致基础上的合作,而且强调通过合作相互强化[28]。

安全情报涉及多个领域,例如在应急情报方面,杨巧云[29]提出利用整体性治理推动政府应急情报协同;在战略情报方面,王馨提出采用差异化协同型的战略情报研究模式[30];在智库情报方面,张海涛等[31]从协同理论的视角对其服务创新机制进行了研究。

在现有的研究中,虽然有部分关于安全情报工作协同的研究涉及了情报流程,但这些研究并没有对安全情报流程的每一个环节中具体的协同工作进行深入分析。此外,在反恐情报领域,现有研究中对反恐情报流程协同的研究较少。从情报流程的视角,按照其环

节对安全情报流程协同进行分析能够详细直观地展现其具体的协同模式。因此,本文以反恐情报工作为例,从情报流程的视角对大数据环境下的安全情报工作协同进行研究。

3 安全情报工作协同的需求分析及存在的问题

3.1 大数据环境下安全情报工作中的协同需求分析

大数据时代,安全情报工作面临数据量大、数据结构多样化、数据来源多样化和数据价值密度低等问题。这些问题贯穿安全情报工作的始终,需要参与安全情报工作的各组织机构共同克服。

协同是大数据环境下提升安全情报工作效率的有效手段。大数据的采集、存储、处理与利用等任务对安全情报工作的硬件条件与软件能力提出了较高要求。安全情报工作中的协同有助于更好地利用大数据信息资源。例如,在使用大数据信息资源时需要配置较高的电脑设备,这增加了安全情报工作的成本。情报工作人员虽然能够获得大量数据,但这些数据真伪难辨,且需要追踪其来源。此外,即使面对同样的数据,不同的情报工作者也可能得出不同的结论,解决这些问题需要情报工作者协同分享经验、能力与智慧。另一方面,大数据并不是全部的数据,在进行大数据分析时,不同的训练集和测试集的选择也会影响最终的结果。通过协同,安全情报工作者能够更加高效地利用大数据资源,获得更准确的分析结果,通过信息与能力共享来提高情报工作效率。

3.2 专业人员短缺

大多数情况下,设计跨组织的协同依赖于组织中特定人员的经验能力[32]。然而,若跨组织的协同依赖于有经验能力的特定人员,将使得组织间难以灵活有效地协同。大数据对安全情报工作协同提出了更高的要求。只有当组织内部的人员能有效利用外部信息时,才能达成协同合作[33]。情报人员应具备的素养与数据的搜集分析方式紧密相关[34]。大数据的数据量大、结构多样化等特点增加了组织内部人员利用外部信息的难度,对情报人员的素养提出了更高的要求。如果组织内部的大部分成员不能理解和利用外部信息,那么组织的协同就只能依赖于组织中少数能够理解利用外部信息的人员。

反恐情报工作也存在专业人员短缺的问题[35]。建立情报中心是一种常见的增加组织协同能力的办法。2015 年颁布的《中华人民共和国反恐怖主义法》指出,要建立国家反恐怖主义情报中心以统筹我国的反恐情报工作,加强各部门合作。随后各省市建立了反恐情报中心,例如 2017 年兰州市对反恐情报综合研判中心进行改造[36],2018 年安徽省启动反恐情报中心系统建设项目[37]。此外,国家安全部、武警和中国人民解放军等部门也涉及反恐业务,其数据库中存储的信息也包含反恐情报。不同数据库的数据存储结构不完全一致,这会增加不同组织共享其获取的情报的成本,使得情报的解读依赖于专业人员。因此,专业人员短缺使得反恐情报工作效率低下,难以及时解决反恐情报工作的困难,满足反恐情报工作的需求。专业人员的培养是一项长期的工作,需要长期的时间投入。因此,反恐情报工作方案需要减少对组织内专业人员的依赖。

3.3 组织之间缺少充分的横向交互

在大数据时代,安全情报所涉及要素的性质、时间、空间、内容和形态处于重构之中[38]。为了提高安全情报工作的效率,有必要从情报流程的视角对安全情报工作协同进行研究。情报流程对于情报工作协同十分重要,情报流程应与其情报需求相匹配。安全情报工作并不是一个单目标的任务,僵化的流程不利于协同工作的展开,因此情报流程的选择至关重要[39-40]。定义情报需求是情报工作的第一步[41]。情报部门之间的横向交互能够更好地满足情报需求[42]。例如,美国情报机构充分调动国家资源,保证情报服务机构与情报需求主体之间信息传递的横向与纵向交互[43]。只有保证各部门之间充分的横向交互,才能提供有价值的安全情报[44]。目前我国在安全情报工作流程中存在横向交互不足的问题[45]。

在反恐情报工作中,尽管情报工作的核心目的是反恐,但在不同情境中反恐情报工作的需求不尽相同。例如恐怖主义事件发生前的反恐情报需求以预防为主,事件发生中的反恐情报需求应当以打击为主。前者属于需求不明确的反恐情报工作,后者属于需求明确的反恐情报工作。可见,反恐情报工作不是一个单目标的任务。反恐情报流程应当能够满足反恐情报预警的需求和针对特定任务的反恐情报工作的需求。因此,为了完成协同,反恐情报流程需要更加灵活,促进各部门的横向交互。只有组织间进行充分的横向交互,才能提高从大数据资源中获得有效情报的效率。因此,反恐情报工作方案需要在满足反恐情报预警的需求和针对特定任务的反恐情报工作需求的基础上,

促进部门间的横向合作。

4 反恐情报协同工作方案构建

4.1 反恐情报主体

为解决第3部分提出的大数据环境下反恐情报工作中协同的问题,本文在整体政府理论[28]的基础上,借鉴美国情报工作外包的模式将社会力量纳入方案中,构建了反恐情报协同工作方案,并从反恐情报主体和主体间具体的协同方式等两个方面进行阐述。该方案中,反恐领导小组对各部门进行协同,专业部门根据具体任务进行反恐情报工作。

在我国全民反恐的背景下,反恐情报工作中情报主体应当包括反恐领导小组、专业部门、一般业务部门和社会力量。根据《中华人民共和国反恐怖主义法》,反恐领导小组统一领导和指挥各部门的反恐情报工作,可以对各部门反恐工作进行协调。专业部门是指中华人民共和国公安部、国家安全部、中国人民武装警察部队和中国人民解放军等拥有专业的反恐情报搜集分析人员,且以反恐作为部门主要任务的组织。一般业务部门是指中国人民银行、中华人民共和国交通运输部、工业和信息化部、海关总署等不以反恐为主要任务,但可以为反恐情报工作提供辅助服务的政府机构。社会力量是重要的反恐情报信息源之一。社会力量包括企业、非营利性组织和群众。其中企业按照所属领域可以划分为金融业、运输业、电信业、服务业、工业等行业。金融业包括银行、证券所等金融机构以及移动支付服务提供商,可以为反恐情报工作提供异常金融流动信息。运输业包括铁路、空运、汽运等,可以为反恐情报工作提供人员流动信息和危险物品运输信息。电信业包括电信、移动、联通等运营商,社交网站运营商和电商,可以为反恐情报工作提供在网上散播恐怖信息的人员名单等。服务业是指酒店、青旅和民宿等,可以为反恐情报工作提供可疑人员的行踪。制造业包括使用或制造危险品的企业,可以为反恐情报工作提供购买危险物品人员的名单。非营利性组织包括公益性团体、权益保护类团体、宗教团体、文教团体等。公益性团体包括非营利性医院、各类基金会等。权利保护类团体包括工会、商会等。宗教团体是指符合法律规定的宗教机构。文教团体包括学校、图书馆、档案馆和博物馆等。非营利性机构同样可以为反恐情报工作提供领域相关的信息,例如非营利性医院可以提供危险传染源信息,商会可以提供业务异常的企业的信息等。参与反恐情报工作的组织按照其职能可以划分为领导层和执行层[46],如表1所示:

表1 反恐情报主体划分

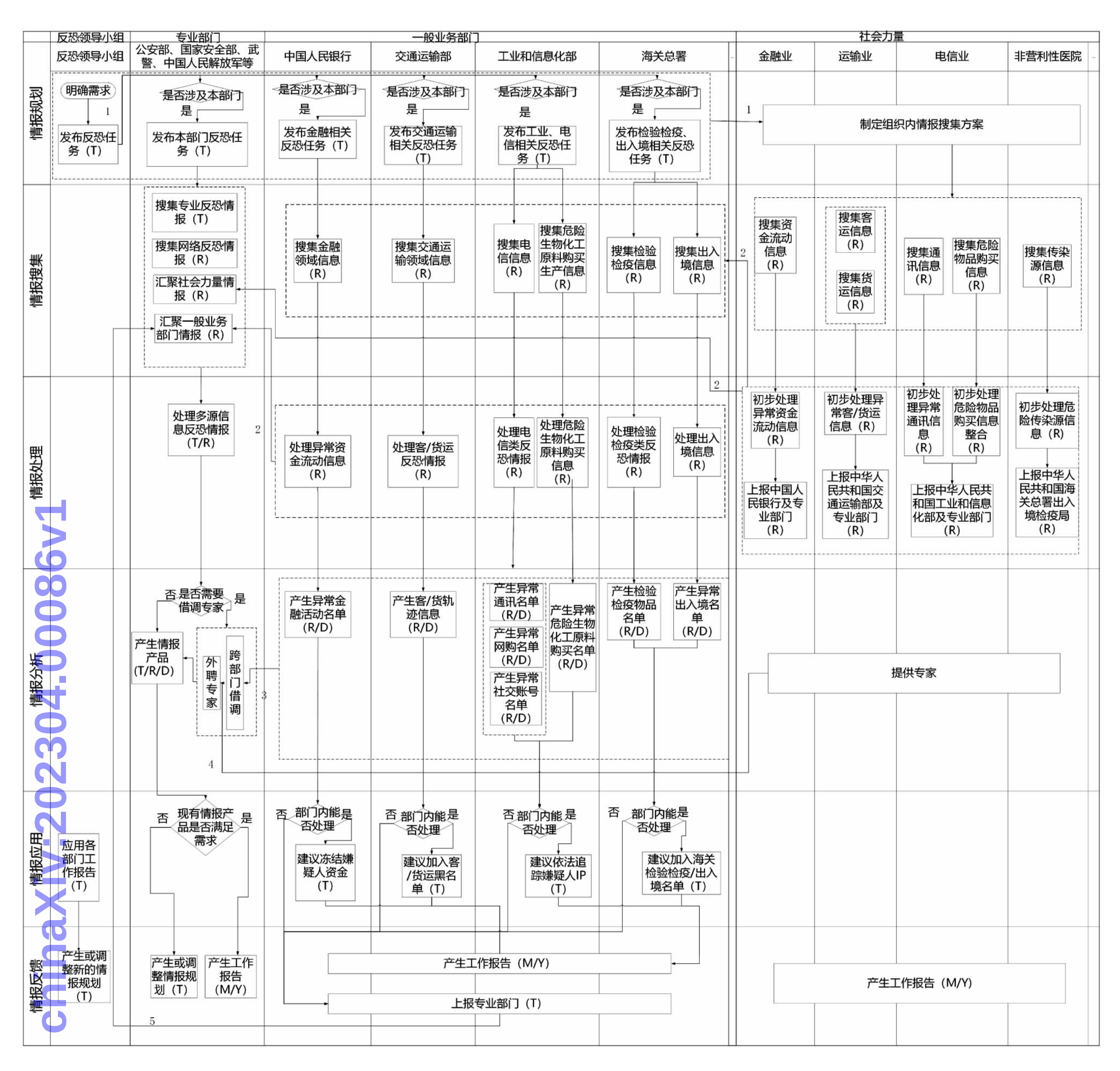
领导层	反恐领导小组	
执行层	专业部门	公安部、国家安全部、中国人民武装警察部队和中国人民解放军
	一般业务部门	中国人民银行、交通运输部、工业和信息化部、海关总署、最高人民法院、最高人民检察院、外交部、财政部、教育部、科学技术部等职能部门
	社会力量	企业:金融业、运输业、电信业、服务业、制造业等行业的企业 非营利性组织:公益性团体、权益保护类团体、宗教团体、文教团体等 群众

4.2 反恐情报工作协同方案

在反恐情报工作中,“协同”意味着反恐情报主体达到优势互补、互利共生。根据4.1节所述的反恐情报主体,本节尝试探讨各反恐情报主体间的协同方案。根据文献[16],按照情报规划、情报搜集、情报处理、情报分析、情报应用与情报反馈等环节构建反恐情报工作协同方案,如图1所示。根据网络交互模型[47]和目标中心模型[48],情报流程的核心应当是明确情报需求或目标,因而在图1中情报流程的起点为“明确需求”。按照多重反复模型[16]和网络交互模型的特点,情报流程间各环节不是固定的流程,而是灵活变化的。当落实到具体的反恐情报任务时,体现为不同情报主体在不同情报环节中的协同,具体协同方式见图1。

数字代表横向交互:1－任务下发;2－呈递已处理的情报;3－借调专家;4－外聘专家;5－上报专业部门。为解决专业人员短缺的问题,本文涉及的反恐情报协同工作方案将一般业务部门和社会力量纳入反恐情报主体,使一般业务部门和社会力量负责部分的情报搜集、情报处理和情报分析工作。此外,通过不同组织间专业人员的相互借调,也可以减少组织对组织内专业人员的依赖。例如政府部门在需要分析金融数据时,可以与金融业界的专业人员或学术界金融领域的专家合作,而不需要专门聘请金融分析师。

为解决组织间缺少充分的横向交互的问题,在本研究提出的反恐情报协同工作方案中,反恐领导小组负责协调各部门的工作,同时各情报主体间进行横向的信息传递。当各情报主体在没有特定的反恐情报任务时,以反恐预警为目的,开展反恐情报工作。在这一情境中,社会力量、一般业务部门和专业部门需在情报搜集和情报处理阶段进行横向交互,传递反恐情报。专业部门在情报分析阶段需和一般业务部门与社会力量进行横向交互,借调专家。当有明确的反恐情报任



注：字母代表频率：T－任务导向；R－实时；M－每月一次；Y－每年一次

图 1　反恐情报工作协同方案

务时，各反恐情报主体在反恐领导小组的领导下开展反恐情报工作。由于专业部门的特殊性，这些部门可以根据特定任务，以任务为导向开展反恐情报工作。例如当公安部需要与交通相关的反恐情报产品时，如果当前的反恐情报产品不能满足公安部的需求，则公安部可以自行制定反恐任务，进行反恐情报工作。

反恐情报流程涉及的部门较多，难以在一张图中完整地呈现，因此在图 1 中选择每类情报主体中的若干部门作为代表。选择中国人民银行、交通运输部、工业和信息化部和海关总署作为一般业务部门的代表；选择金融业、运输业和电信业作为社会力量中企业的代表；选择非营利性医院作为社会力量中非营利性组织的代表。

4.2.1　情报规划阶段的协同

情报规划是对整个情报工作进行规划的过程[49]。情报规划工作应当基于情报需求展开，对情报工作过程中各组织的职责进行划分，确定各组织的情报工作目标。大数据环境下，各部门在反恐情报工作中需要面对的数据类型繁多、数量庞杂。可用于反恐情报工作的数据在类型上包括音频数据、视频数据和文字等多种形式，而其数据来源也包括移动通信数据、商业交易数据和传感器数据等多种源头。这些数据分布于不

同的部门。明确的反恐情报规划有助于各部门明确职责,结合实际展开反恐情报工作。例如美国的国家情报总监能够对全国的情报机构进行协调管理,能够明确各机构在反恐情报工作中的任务[50]。

在图1中,反恐领导小组在明确需求后,制定宏观的情报规划,以通知公告、政策制度等形式发布反恐情报任务。专业部门和一般业务部门根据宏观的情报规划,结合部门实际情况制定具体的情报规划,以通知公告、政策制度等形式发布反恐情报任务。例如,反恐领导小组发布网络反恐情报搜集的任务,工业和信息化部根据该反恐情报规划调整网络情报规划,例如搜集社交媒体中发布异常信息的帐号。社会力量包括企业、非盈利性组织等具有复杂结构的组织,在进行情报搜集工作时也需要考虑组织内各部门的分工,因而社会力量需要根据反恐领导小组的任务和各上级主管部门发布的反恐任务,以工作方案或组织内部制度的形式,生成组织内反恐情报搜集方案。在进行情报规划后,情报主体根据具体的规划进行情报搜集工作。

由反恐领导小组制定宏观规划,其余组织结合自身实际情况细化反恐情报规划的情报规划方式能够明确各组织的责任,保证情报规划的可操作性,提高协同效率。

4.2.2 情报搜集阶段的协同

情报搜集是指依照情报规划获取情报信息。大数据情境下情报搜集环节需要使用多种信息源。反恐情报搜集的信息来源既有非公开的信息源,也有公开的信息源。非公开的信息包括政府部门内部的保密信息、未公开的商业信息、专业的情报人员搜集的信息等,公开的信息包括网络信息和各组织主动对外公开的信息等。

反恐情报搜集不应只是治安维护部门的职责,反恐情报搜集工作同样需要多个部门的参与配合。专业部门既可以通过公开的信息源进行反恐情报搜集工作,也可以通过非公开的信息源进行反恐情报搜集工作。而一般业务部门和社会力量则在开源信息搜集中扮演着重要的角色。例如,恐怖主义行动往往需要用到炸药、枪支等武器。恐怖分子会通过购买、盗窃等手段获取炸药等武器,搜集危险物品的购买、运输信息有助于提前发现恐怖分子[51]。而将一般业务部门和社会力量纳入反恐情报体系,就可以提供相关情报。例如工信部可以通过搜集汇总电信业提供的危险物品购买名单,发现恐怖分子囤积炸药、枪支的行为。交通部可以通过搜集汇总运输业提供的客运、货运名单发现恐怖分子异常的人员流动和武器运输。

在情报搜集阶段,一般业务部门需要搜集社会力量初步处理过的反恐情报。专业部门搜集一般业务部门和社会力量的反恐情报,同时进行任务导向的情报搜集和网络情报搜集。

社会力量对行业内的信息进行搜集并存储在组织内的业务数据库中以便后续的情报处理工作。金融业实时搜集资金流动信息。运输业实时搜集客运信息和货运信息。电信业实时搜集通讯信息和危险物品购买信息。非营利性医院实时搜集传染源信息。当发现反恐情报时,社会力量需要及时记录,因而频率为实时。

一般业务部门对所辖领域的信息进行搜集并存储在部门内的业务数据库中以便后续的情报处理工作,频率为实时。中国人民银行搜集金融领域信息。交通运输部搜集汇总交通运输领域信息。工业和信息化部搜集电信信息和危险生物化工原料购买信息。海关总署搜集检验检疫信息和出入境信息。

专业部门需要搜集多种信息并存储在部门内的反恐数据库中以便后续的情报处理工作,以任务为导向进行专业情报搜集工作,即让专业的情报工作者进行人力反恐情报搜集。同时专业部门需要搜集网络反恐情报,频率为实时。此外,专业部门需要汇聚一般业务部门和社会力量的信息,频率为实时。实时搜集反恐情报有利于提高反恐情报工作的效率,大数据和互联网能够实现数据的实时搜集和传递。

各组织的日常业务本就涉及行业内数据的搜集,由各组织搜集所处领域的数据一方面可以保证数据搜集人员的专业性,一方面可以减少重复的数据搜集工作,充分发挥各组织的优势。

4.2.3 情报处理阶段的协同

情报处理是对搜集的数据进行加工的过程。其中包括对数据真伪的辨别,对数据价值的判断和对数据的整合及序化[16]。大数据情境下,大量数据真假难分,反恐情报工作的情报处理阶段应当起到对海量数据去伪存真的作用。例如网络中的信息数据量庞大,但其中存在许多“垃圾信息”。这些“垃圾信息”可能是相互矛盾的信息,也可能是与反恐工作无关的信息。在情报处理阶段,就需要对信息进行清洗,去除“垃圾信息”,保留有效信息,并统一数据的存储格式,以便后

续进行情报分析工作。

在反恐情报处理过程中,情报处理者并不是唯一的,而是分布在多个部门,甚至多个区域的机构。专业部门应当承担主要的情报处理工作,但一般业务部门和社会力量在负责情报搜集工作之余也会涉及简单的情报处理工作,对数据进行初步的价值判断和分类。例如为了对嫌疑人的行动轨迹进行预测,在情报处理阶段运输业需要对客运、货运信息进行初步处理,包括删除重复信息、序化数据结构并对数据进行整合。而交通部需要对各运输企业递交的客运、货运信息进行进一步的处理,包括对数据价值的判断、删除重复的信息、整合不同地区和企业递交的客运、货运信息。为了更好地进行协同,各情报主体在进行情报处理时,应当使用相同的数据存储结构。

在情报处理阶段,社会力量对搜集到的情报实时进行处理,并将处理后的数据实时上报给一般业务部门和专业部门。一般业务部门对各地上报的情报进行进一步的处理,并将处理后的数据实时上报专业部门。公安部、国家安全部、武警和中国人民解放军等专业部门实时处理多源反恐情报,或以任务为导向进行情报处理工作。利用信息技术实现对数据的自动处理,从而实现对数据的实时处理,将处理后的数据存储在相关数据库中。一般业务部门和专业部门在对情报进行处理后,进入情报分析阶段。社会力量在对情报进行处理后,进入情报反馈阶段。若专业部门有外聘专家的需求,社会力量可在情报分析阶段选拔领域专家推荐给专业部门。

社会力量、一般业务部门拥有行业内的专家。通过上述的情报处理方式,可以充分地利用这些专家,减少专业部门的工作量,提高整体工作效率。

4.2.4 情报分析阶段的协同

情报分析是指结合情报需求利用情报分析工具对数据进行分析形成情报产品的过程[52]。通过情报分析,我们应当能够得到一些区别于原数据的情报[53]。

在大数据时代以前,开源信息由于数据量大难以被应用到统计分析中。而随着技术的进步,通过大数据分析可以精准地分析恐怖分子的活动,开源信息和政府部门的业务信息都可以用于大数据分析。不同的数据应当选择不同的情报分析方法。例如对于小数据,可以选择传统的统计分析方法。对于大数据,可以选择聚类、分类等方法对恐怖分子的行动轨迹、武器流通动向进行预测,或对恐怖分子的身份进行识别。同时,也可以利用深度学习的方法对音频、视频和文字类型的数据进行分析。例如可以利用卷积神经网络(CNN)或递归神经网络(RNN)对恐怖分子的照片、监控录像等图像进行识别,与已有的恐怖分子照片进行比对,以识别恐怖分子。在实际应用中,美国借助大数据开发了乘客筛选系统,能够提供可疑乘客的名单,帮助航空业筛选排查恐怖分子[54]。

情报分析产出的结果依赖于情报分析人员的能力。情报产品的质量也会受到情报人员思维方式、专业背景的影响,正如一位优秀的金融分析师不能胜任军事情报的分析。而通过专家借调可以更好地进行情报分析工作。例如美国在进行反恐情报工作时会从学术界和业界雇佣专家进行短期的情报分析工作[55]。

专业部门首先判断是否需要借调专家。如果不需要借调专家则直接产出情报产品。如果需要借调专家,则通过与一般业务部门协同,实现跨部门的专家借调;或者与社会力量协同,采取外聘专家的方式。例如,当分析金融类反恐情报时,专业部门可与中国人民银行的金融专家以及高校、证券投资所的专家合作。一般业务部门则只对本领域的情报进行分析。中国人民银行产生异常金融活动名单,交通运输部产生客运、货运轨迹信息,工业和信息化部产生异常通讯名单、异常网购名单、异常社交账号名单、异常危险生物化工原料购买名单,海关总署产生检验检疫物品名单和异常出入境名单。

专业部门产出情报产品的频率为以任务为导向、实时和每日。一般业务部门产出情报产品的频率为实时和每日。专业部门有以任务为导向的情报工作,因而专业部门的情报分析的频率包括以任务为导向。通过人工智能等算法可以实现实时的情报分析。专家每日进行人工的情报分析。一般业务部门和专业部门在对情报进行分析后,进入情报应用阶段。

在情报分析阶段,专业部门与一般业务部门和社会力量进行协同,通过专家借调能够减少专业部门对组织内专家的依赖。

4.2.5 情报应用阶段的协同

情报应用是利用情报产品辅助决策的过程。反恐情报应用即是利用反恐情报产品辅助情报用户进行包括反恐行动部署、反恐工作规划等工作在内的决策的过程。

反恐情报工作中专业部门使用情报产品的方式可以分为两类[56]:①使用以需求为导向进行情报活动产生的情报产品。美国为打击阿富汗的恐怖组织而预先派遣人员深入阿富汗进行情报工作[57],这就属于以需求为导向进行的情报活动。②专业部门在现有的情报产品中进行选择。在大数据的情境下,专业部门可以利用反恐数据库或相关部门的业务数据库从各类情报产品中进行选择。例如当公安部门需要犯罪嫌疑人的轨迹信息时,可以与交通运输部门合作,从交通运输部的业务数据库中进行查询。这些情报产品可能是以前的以需求为导向的情报活动产生的情报产品,也可能是在需求不明确的情况下,情报生产者根据自己所处的领域生产的情报产品。人民银行产生的异常金融活动名单就属于情报生产者根据自己所处的领域生产的情报产品。

在情报应用阶段,一般业务部门首先判断部门能否处理该事件。若该事件超出一般业务部门的处理范围,一般业务部门应积极与专业部门合作,呈递相关反恐情报。例如当工业和信息化部通过应用危险生物化工原料购买名单和异常通讯名单发现嫌疑人时,应积极主动与专业部门沟通,呈递嫌疑人名单。

反恐领导小组应用各部门的工作报告。专业部门首先判断现有情报产品能否满足情报需求。现有情报产品若满足需求则直接应用。如果现有情报产品不能满足需求,则进行反馈,生成或调整情报规划。一般业务部门判断部门内能否完成该任务,若不能完成则上报专业部门。部门内若能够完成,则自行处理。例如,中国人民银行可根据前述情报分析,产生冻结嫌疑人资金的建议;交通运输部考虑将嫌疑人加入客运、货运黑名单;工业和信息化部考虑依法对嫌疑人进行 IP 追踪;海关总署考虑将传染源加入检验检疫物品名单,或将嫌疑人列入异常出入境名单。社会力量应用各类政策规章,对情报搜集、处理过程进行相应调整。一般业务部门和专业部门在对情报进行应用后,进入情报反馈阶段。

在情报应用阶段,通过一般业务部门与专业部门的横向交互,将一般业务部门不能处理的反恐情报任务移交专业部门,能够实现反恐情报任务的合理分配,提高反恐情报工作的整体效率。

4.2.6 情报反馈阶段的协同

情报反馈贯是指情报工作执行后产生的反馈信息。这种反馈的信息将再进一步对情报流程的各个环节进行调整。在大数据情境下,可以利用数据库记录每一次反恐情报工作的具体实施方案及反馈。成功的反恐情报工作能够为之后的相同类型反恐情报工作提供一种可行的工作模式。反馈的信息也能为之后的反恐情报工作提供参考。

在图 1 的情报反馈阶段,反恐领导小组以任务为导向产生或调整情报规划。专业部门在现有情报产品满足或不满足需求时以任务为导向产生或调整情报规划,对本次任务的情报应用情况进行总结,以对下一次的情报规划进行调整。在现有情报产品满足需求时,产生月度工作报告及年度工作报告。一般业务部门若不能处理该事件则上报专业部门;若能够处理该事件,则以月度工作报告及年度工作报告的形式进行反馈。社会力量产生月度工作报告及年度工作报告。月度工作报告用于总结当月的情报应用情况,以对中短期的情报规划进行调整。年度工作报告用于总结当年的情报应用情况,以对长期的、宏观的情报规划进行调整。社会力量根据政策规章调整反恐情报搜集方案。在情报反馈完成后,各情报主体又进入了情报规划阶段。

在情报反馈阶段包括以任务为导向的情报反馈和定期的情报反馈,结合这两种情报反馈方式能够及时发现反恐情报规划的不足,并及时调整各组织的反恐情报任务,有利于各组织达到优势互补、互利共生的目的。

5 大数据环境下安全情报工作协同前景展望

大数据具有数据量大、数据类型多样的特点。通过构建大数据环境下反恐情报工作方案,能够对安全情报工作的前景进行展望。为了构建协同的安全情报工作方案,未来的安全情报工作应注重以下 3 点:

5.1 加强信息资源共享与交流

因为大数据具有数据量大的特点,所以在利用大数据时,情报工作会更加繁重。在大数据环境下的安全情报工作中加强信息资源共享与交流能够减少重复的工作,提高整体工作效率并节省情报工作成本。为了构建一个在大数据环境下能够达到良好协同效果的反恐情报工作方案,在上述反恐情报工作方案中,通过增强反恐领导小组、专业部门、一般业务部门和社会力量之间的交流加强了各情报主体间的信息资源共享与

交流。在安全情报工作中应注重加强各情报主体间的交流,对安全情报信息进行整合,以避免"信息孤岛"现象,能够节省对大量数据进行搜集、处理和分析等工作的时间,提升整体工作效率。

5.2 加强情报服务外包

大数据的数据量大,但数据价值低,部分大数据的搜集和处理工作价值较低。在安全情报工作中加强情报服务外包能够避免组织内的重复工作,减少低价值工作。在上述反恐情报工作方案中通过将部分反恐情报搜集和处理的任务分配给一般业务部门和社会力量,减轻了专业部门的工作压力,使专业部门能够将资源更多地用于专业性更强、要求更高的任务,提高了整体的资源利用效率。在安全情报工作中,将部分任务外包给其他的机构或组织,能够减少本组织的低价值活动,将更多的资源用于价值更高的活动中,能够提高组织的工作效率。

5.3 规范情报工作模式

单个的组织对数据的处理能力是有限的,在大数据环境下,为了提高数据的利用效率,可能会有更多的组织通过合作或服务外包的形式参与安全情报工作。规范情报工作模式能够使得情报工作中的参与者权责分明,有利于安全情报工作的纠错和自我完善。在本文构建的反恐情报工作方案中通过反恐领导小组明确参与者的责任,并在情报反馈后对情报工作进行纠错,使得反恐情报工作能够及时发现、解决问题。在安全情报工作中,应当规范情报工作的模式,明确参与者的责任,避免发生相互推诿工作的情况,有助于发现安全情报工作模式中的漏洞并进行调整。

6 结语

安全情报工作有助于统筹外部安全和内部安全,识别并防范安全风险,维持社会稳定。大数据环境与技术给安全情报工作既提出挑战也带来机遇。本文以安全情报中的反恐情报工作为例,探索大数据环境下安全情报工作的协同方案。

本文首先分析了安全情报工作协同面临的两个问题,并针对反恐情报对这两个问题进行具体分析,指出协同的防控情报工作方案应满足以下条件:减少对组织内专业人员的依赖;在满足反恐情报预警的需求和针对特定任务的反恐情报工作的需求基础上促进部门间的横向合作。针对反恐情报工作协同的问题,明确反恐情报工作中的情报主体,即反恐领导小组、专业部门、一般业务部门和社会力量,从情报流程的视角提出了在反恐领导小组发布的反恐情报任务指引下专业部门、一般业务部门和社会力量协同合作的反恐情报工作协同方案。选择中国人民银行、交通运输部、工业和信息化部和海关总署代表一般业务部门;选择金融业、运输业和电信业代表社会力量中的企业;选择非营利性医院代表社会力量中的非营利性组织,对反恐领导小组、专业部门、一般业务部门和社会力量在反恐情报工作中的具体协同方式进行了阐述。本文提出的反恐情报工作协同方案有助于减少组织对内部专业人员的依赖并促进组织间的横向交互,提高反恐情报工作效率,降低反恐情报工作的成本。本研究能够为提高反恐情报工作成效提供可行方案。此外,在研究中考虑了大数据对反恐情报工作的影响,从情报流程的视角论述了大数据环境下反恐情报工作的协同方式,能够为大数据环境下的安全情报工作协同研究提供参考。

参考文献:

[1] 王秉,吴超. 安全情报在安全管理中的作用机理及价值分析[J]. 情报理论与实践,2019,42(2):38-43.
[2] 张家年. 国家安全保障视域下安全情报与战略抗逆力的融合与对策[J]. 情报杂志,2017,36(1):1-8,22.
[3] 王英,王涛. 我国网络与信息安全政策法律中的情报观[J]. 情报资料工作,2019,40(1):15-22.
[4] WANG Y, LIU Y, CANEL C. Process coordination, project attributes and project performance in offshore-outsourced service projects [J]. International journal of project management, 2018, 36(7): 980-991.
[5] 王秉,吴超. 安全情报概念的由来、演进趋势及涵义——来自安全科学学理角度的思辨[J]. 图书情报工作,2019,63(3):45-53.
[6] 都伊林,吴骁. 智慧城市视角下完善反恐预警机制研究[J]. 情报杂志,2015,34(7):13-17,33.
[7] 蔡士林. 美国国土安全事务中的情报融合[J]. 情报杂志,2019,38(1):8-12,18.
[8] 李恒,邓峰彬. 国家安全视阈下反恐情报信息应用价值与法治实践[J]. 中国刑警学院学报,2019(1):28-35.
[9] 肖连杰,孟涛,王伟,等. 基于深度学习的情报分析方法识别研究——以安全情报领域为例[J]. 数据分析与知识发现,2019,3(10):20-28.
[10] 王秉,吴超. 情报主导的安全管理(ILSM):依据、涵义及模型[J]. 情报理论与实践,2019,42(6):56-61.
[11] 高金虎. 试论国家安全情报体制的改革路径[J]. 公安学研究,2019,2(2):1-26,123.

［12］章雅蕾,吴超,王秉. 安全情报素养:总体国家安全观背景下安全人员的必备素养［J］. 情报杂志,2019,38(3):33－38,113.
［13］吴超,吴林. 安全情报视域下安全管理模式探讨［J］. 广州大学学报(社会科学版),2020,19(2):25－32.
［14］秦殿启,张玉玮. 情报素养:信息安全理论的核心要素［J］. 情报理论与实践,2015,38(4):30－33.
［15］李辉,陈雪飞,刘如,等. 国家安全与发展视阈下情报供给侧改革研究——基于供给侧五角模型解释框架［J］. 情报理论与实践,2019,42(10):9－14.
［16］洛文塔尔. 情报:从秘密到政策［M］. 杜效坤,译. 北京:金城出版社,2015.
［17］张家年,卓翔芝. 融合情报流程:我国智库组织结构和运行机制的研究［J］. 情报杂志,2016,35(3):42－48.
［18］CAO G, DUAN Y, CADDEN T. The link between information processing capability and competitive advantage mediated through decision-making effectiveness［J］. International journal of information management, 2019, 44: 121－131.
［19］彭知辉. 情报流程研究:述评与反思［J］. 情报学报,2016,35(10):1110－1120.
［20］CHAKRABORTY R, AGRAWAL M, RAO H R. Information processing under stress: a study of Mumbai police first responders［J］. IIMB management review,2014,26(2):91－104.
［21］WILLIOT A, BLANCHETTE I. Can threat detection be enhanced using processing strategies by police trainees and officers? ［J］. Acta psychologica,2018,187: 9－18.
［22］李建辉,陈俊旭,单一唯. 大数据对公安情报流程影响研究［J］. 湖北警官学院学报,2015(3): 20－23.
［23］BARTES F. Counter competitive intelligence cycle［C］//KOCOUREK A. Proceedings of the 11TH international conference on liberec economic forum 2013. Liberec: Technical University Liberec,2013:18－26.
［24］MALONE T W,CROWSTON K G. What is coordination theory and how can it help design cooperative systems［C］//HALASZ F. Proceeding of the 1990 ACM conference on computer-supported cooperative work. New York: ACM,1990: 357－370.
［25］MU W, BÉNABEN F, PINGAUD H. Collaborative process cartography deduction based on collaborative ontology and model transformation［J］. Information sciences, 2016, 334: 83－102.
［26］弋亚群,刘益,李垣. 组织资源的协同机制及其效应分析［J］. 经济管理,2003(16):12－16.
［27］许学国. 组织协同学习机理及实证研究［J］. 系统管理学报,2010,19(3):284－297,322.
［28］PERRI 6. Joined-up government in the western world in comparative perspective: a preliminary literature review and exploration［J］. Journal of public administration research and theory, 2004, 14(1):103－138.
［29］杨巧云. 整体性治理视域下的应急情报体系协调研究［J/OL］. 情报理论与实践.［2020－04－20］. http://kns. cnki. net/kcms/detail/11. 1762. G3. 20190821. 1113. 002. html.
［30］王馨. 战略情报研究模式反思与探索:计划、动态还是协同［J］. 情报理论与实践,2013,36(8):1－5.
［31］张海涛,张念祥,王丹,等. 大数据背景下智库情报的服务创新——基于协同理论视角［J］. 现代情报,2018,38(9):57－63.
［32］MONTARNAL A, MU W, BENABEN F, et al. Automated deduction of cross-organizational collaborative business processes［J］. Information sciences, 2018, 453: 30－49.
［33］孙凯,刘人怀. 基于信息处理理论的跨组织信息共享策略分析［J］. 管理学报,2013,10(2):293－298.
［34］李品,杨建林. 基于大数据思维的情报学科发展道路探究［J］. 情报学报,2019,38(3):239－248.
［35］翟家圣. 公安院校反恐人才培养探析——以中国刑事警察学院为例［J］. 云南警官学院学报,2017(5):46－50.
［36］中国政府采购网. 兰州市公安局全市反恐情报综合研判中心改造工程和设备购置项目中标公告［EB/OL］.［2020－04－20］. http://www. ccgp. gov. cn/cggg/dfgg/zbgg/201710/t20171017_8996726. htm.
［37］安徽省政府采购网. 安徽省公安厅省级反恐情报中心系统建设［EB/OL］.［2020－04－20］. http://www. ccgp-anhui. gov. cn/cmsNewsController/cmsNewsDetail. do? newsId = 0d6c35a3-e886-41be-8c6f-067f3f35a2fc.
［38］王世伟. 论大数据时代信息安全的新特点与新要求［J］. 图书情报工作,2016,60(6):5－14.
［39］BARTHE-DELANOË A, MONTARNAL A, TRUPTIL S, et al. Towards the agility of collaborative work flows through an event driven approach-application to crisis management［J］. International journal of disaster risk reduction,2018,28:214－224.
［40］化柏林,李广建. 面向情报流程的情报方法体系构建［J］. 情报学报,2016,35(2):177－188.
［41］NAJAFI-TAVANI S, NAJAFI-TAVANI Z, NAUDÉ P, et al. How collaborative innovation networks affect new product performance: product innovation capability, process innovation capability, and absorptive capacity［J］. Industrial marketing management, 2018, 73:193－205.
［42］李晓东. 情报体制在联合作战情报需求问题上的影响初探［J］. 情报杂志,2010,29(S2):111－113,110.
［43］张志华,张凌轲. 基于网络信息安全的国家竞争情报战略研究:以美国为例［J］. 图书馆理论与实践,2016(8):36－41,76.
［44］汤世国. 当代科学的整体化趋势与情报科学的形成［J］. 情报科学,1982(2):8－12.
［45］徐向华,刘志欣. 上海环境风险应急管理制度检讨及立法完善［J］. 法学杂志,2011,32(S1):169－174.
［46］安璐,周亦文,杨羽茜. 反恐情报工作协同组织架构研究［J］. 情报理论与实践,2019,42(8):17－24.

[47] U. S. Joint chiefs of staff. Joint publication 2 - 01, joint and national intelligence support to military operations[R]. Washington D. C.: GPO, 2004: III - 2.
[48] CLARK M R. Intelligence analysis-a target-centric approach[M]. Washington D. C.: CQ Press, 2006:10 - 15.
[49] 季建超,司有和,翟伟希,等. 企业竞争情报工作过程与企业绩效的相关性分析[J]. 现代情报,2011,31(5):123 - 126.
[50] 袁莉,姚乐野. 应急管理中的"数据 - 资源 - 应用"情报融合模式探索[J]. 图书情报工作,2014,58(23):26 - 32.
[51] 贾宇,李恒. 恐怖犯罪活动组织和人员之情报信息搜集研究[J]. 情报杂志,2017,36(2):32 - 39.
[52] 段晨杰. 公安情报分析工作面临的困境及应对措施[J]. 情报探索,2018(12):87 - 91.
[53] LANGEFORS B. Infological models and information user views[J]. Information systems, 1980,5(1): 17 - 32.
[54] 金波,杨涛,吴松洋,等. 电子数据取证与鉴定发展概述[J]. 中国司法鉴定,2016(1):62 - 74.
[55] 孙宗义,赵金萍. 美国情报界私人公司的情报承包机制研究[J]. 情报杂志,2016,35(3):49 - 53.
[56] 刘如,李梦辉,张惠娜,等. 意愿经济环境下用户情报需求的深度挖掘与探索[J]. 图书情报工作,2017,61(1):14 - 24.
[57] 彭亚平. 有感美国情报工作在反恐战争中的作用[J]. 国家安全通讯,2002(4):30 - 31.

作者贡献说明:

安璐:研究思路设计,论文修改;
周亦文:论文撰写及修改。

Research on the Collaboration of Security & Safety Intelligence Work in the Big Data Environment
——Taking Counter-Terrorism Intelligence Work as an Example

An Lu[1,2] Zhou Yiwen[2]
[1] Center for Studies of Information Resources, Wuhan University, Wuhan 430072
[2] School of Information Management, Wuhan University, Wuhan 430072

Abstract: [**Purpose/significance**] Big data puts forward high requirements for security & safety intelligence work collaboration. A study on the problems and solutions in security & safety intelligence work collaboration is helpful for departments related to security & safety intelligence to work together and to improve the effectiveness of security & safety intelligence work. [**Method/process**] This paper discussed the possible problems of security & safety intelligence cooperation under the big data environment. Taking counter-terrorism intelligence as an example, combined with the process of intelligence work, it analyzed the main body and cooperation needs of security & safety intelligence work, and put forward the cooperation scheme of counter-terrorism intelligence work. [**Result/conclusion**] Under the guidance of the counter-terrorism intelligence demand issued by the counter-terrorism leading group, the Ministry of Public Security and other professional departments cooperate with the People's Bank of China, the Ministry of Transportation, the Ministry of Industry and Information Technology, the General Administration of Customs and other general business departments, as well as the financial, transportation, telecommunications, and medical industries and non-profit sectors, the masses and other social forces to collect, process, analyze, apply and deliver counter-terrorism intelligence in specific fields.

Keywords: security & safety intelligence counter-terrorism intelligence collaboration intelligence processes big data